GNSS Positioning Security: Automatic Anomaly Detection on Reference Stations

Stéphanie Lebrun^{1,2} , Stéphane Kaloustian¹ , Raphaël Rollier¹ ,
and Colin Barschel²

¹ Swisstopo, 3084 Wabern, Switzerland

{stephane.kaloustian,raphael.rollier}@swisstopo.ch

² Cyber Defence Campus - Armasuisse, 3602 Thun, Switzerland
colin.barschel@armasuisse.ch

Abstract. The dependency of critical infrastructures on Global Navigation Satellite Systems (GNSS) keeps increasing over the years. This over-reliance brings concerns as those systems are vulnerable and consequently prone to human-made perturbations, such as jamming and spoofing attacks. Solutions for detecting such disturbances are therefore crucially needed to raise GNSS users' awareness and protection. This paper suggests an approach for detecting anomalous events (i.e., potentially an attack attempt) based on measurements recorded by Continuously Operating GNSS Reference Stations (CORS). Precisely, the anomaly detection process first consists in modeling the normal behavior of a given signal thanks to a predictive model which combines the *Seasonal and Trend decomposition using LOESS* and *ARIMA* algorithms. This model can then be used to predict the upcoming measurement values. Finally, we compare the predictions to the actual observations with a statistical rule and assess if those are normal or anomalous. While our anomaly detection approach is intended for real-time use, we assess its effectiveness on historical data. For simplicity and independence, we also focus on the *Carrier-to-Noise Ratio* only, though similar methods could apply to other observables. Our results prove the sensitivity of the proposed detection on a reported case of unintentional disturbance. Other anomalies in the historical data are also uncovered using that methodology and presented in this paper.

Keywords: GNSS · CORS · RINEX · Jamming · Spoofing · Anomaly detection · Carrier-to-Noise Ratio · Critical infrastructure protection

1 Introduction

The Global Navigation Satellite Systems (GNSS) refer to groups of artificial satellites enabling a user to determine its position and time, anywhere and any-time on Earth. Today, almost every mode of transportation relies on GNSS, including aviation, maritime, and railway sectors [1]. Moreover, navigation satellites carry on board atomic clocks, all synchronized to a master clock. This

precise source of timing provides a reference for a range of processes in telecommunication networks, electrical power grids, and financial transactions [2, 3]. It is also a critical component in rescue operations, for instance, to locate the source of an incident [4]. Due to their global availability, performance, ease of use, and low cost, GNSS are the preferred - and often unique - source of navigation and timing information in many critical applications.

Nevertheless, GNSS are increasingly targeted by cyber-attacks (e.g., [6, 7]). The ability to automatically detect and report such events is vital to ensure a continuity of navigation service and identify the sources of disruption.

Since the growth in popularity of satellite navigation, many countries have established a network of Continuously Operating Reference Stations (CORS) to enhance GNSS activities. AGNES¹ is one such CORS network comprising 31 GNSS static stations distributed across Switzerland. The purpose of this paper is to investigate whether the data that these stations continuously collect could contribute to the automatic real-time detection of potentially malicious events.

It is noteworthy that this research does *not* intend to provide the one solution to all GNSS security issues, nor to cover a specific scenario of attack. It rather aims at contributing to the general security enhancement of GNSS users by monitoring signal parameters and providing information on detected anomalies.

The anomaly detection scheme we propose works as follows. Each station continuously tracks GNSS satellites from multiple constellations and transmits signal measurements. Since the stations are static, some of the measurements, e.g., the *Carrier-to-Noise Ratio*, have a predictable behavior at a given station. Therefore, a signal measurement patterns can be learned by fitting a predictive model on past data. Hence, the model can predict future values accurately. Next, the actual values of the given measurement are compared to the predicted ones. Using a statistical rule based on how well the model usually predicts, we can assess whether the observed values are normal or anomalous. An anomaly may indicate the occurrence of an attack around the station or some other kind of malfunction possibly impacting GNSS users.

To study the feasibility of such a scheme, in this research, we work on the historical data of the *Carrier-to-Noise Ratio* parameter recorded in so-called RINEX files for two constellations (GPS and GLONASS) by different stations. One reported case of disturbance allows confirming the anomaly detection is effective. Then, we discover other anomalous events.

In comparison to related work, our approach presents two significant benefits. Its simplicity first, as our only assumption is that the stations are static. Second, we leverage high-level information available on every GNSS receiver. Therefore, the same methodology applies to any other static GNSS receiver without the need for new hardware.

The remainder of this paper consists of six sections. Section 2 reviews the basic principles behind GNSS technology and its vulnerabilities. Related work is then discussed in Sect. 3. Next, the methodology proposed to detect anomalies in an automated way is outlined in detail in Sect. 4. The results are presented

¹ Automated GNSS Network for Switzerland.

in Sect. 5. Limitations and future work are discussed in Sect. 6. The final section summarizes the paper and draws its conclusions.

2 Background Theory on GNSS

In this section, we briefly present the basics of GNSS technology and its principal vulnerabilities.

2.1 Technology Basics

GNSS are groups of satellites (*constellations*) continuously sending signals to the Earth, allowing positioning and timing services over a wide geographical area. Today, four systems provide global coverage: the American GPS, the Russian GLONASS, the European Galileo, and the Chinese BeiDou. The principle of operation remains the same across all systems and is illustrated in Fig. 1. Each transmitted signal encodes a Navigation Message from which the satellite's position at a given time can be determined (quantity (a) in Fig. 1). Then, other signal characteristics, e.g., propagation time, allow computing the distance between the satellite and the receiver (quantity (b)). Given that information for at least four satellites, the receiver can derive its position (quantity (c)) and adjust its clock.

Fig. 1. Satellite-based positioning principle. Adapted from [8].

For each constellation, multiple parts of the L-band (which ranges from 1 GHz to 2 GHz) are allocated for the satellites to transmit their signals at different frequencies.

Upon the reception of a signal, the receiver measures and records the *Carrier-to-Noise Ratio* (C/N_0). It consists of the ratio of the received desired satellite signal power to the noise power per unit bandwidth. It is often used to measure signal quality and the noise environment of GNSS observations [9].

The C/N_0 and other signal measurements are commonly stored at a receiver in files written under the standard human-readable format named Receiver Independent Exchange Format (RINEX).

2.2 Vulnerabilities

GNSS signals may experience perturbations that are *naturally* or *intentionally* entailed [10]. Regarding the latter, two well-known malicious actions can harm a GNSS user, namely *jamming* and *spoofing*. Jamming refers to the intentional emission of interference to prevent the processing of legitimate signals and deny the availability of GNSS service [11]. Due to the long distance they travel, signals reach the ground receivers with a low power level and can be easily overshadowed. On the other hand, a spoofing attack can occur because *civilian* GNSS signals (in contrast to signals in military use) are neither encrypted nor authenticated, and the signal's specifications are publicly available [12]. It is then possible for an attacker to impersonate a satellite and transmit counterfeit signals, misleading a receiver to compute a wrong position or time [13]. One way to achieve a spoofing attack in spite of encryption is to acquire an authentic signal and to replay it with some delay or from another location [14]. This type of spoofing is referred to as *meaconing*.

It should be noted that GNSS service providers are currently developing solutions against spoofing that rely on cryptographic mechanisms (e.g., Galileo OS-NMA, PRS, GPS CHIMERA) [15, 16]. For example, the cryptographic authentication of GNSS signals would ensure a user that they were generated by a satellite [15]. While this is an important step towards greater security for GNSS users, this approach may not protect against meaconing since authentic signals are re-broadcasted [17]. Moreover, such systems are not fully operational yet. In any case, we believe that there is no silver-bullet solution to the threats against GNSS. Therefore, any means of detection may contribute to increase the protection by rising the awareness level in case of disturbance.

2.3 Attacks Incentives

From fraud to terrorism, the motivations for initiating an attack against GNSS are numerous. Both theory and practice demonstrated the feasibility of the attacks described in the previous section.

For example, in 2011, Iranian forces captured a flying US drone by spoofing it to spy on the drone's technology [18]. For terrorist purposes, an attacker could also consider steering off the course of a larger vehicle, such as a ship. The workability of such a scenario was demonstrated by [19], and several reported real-world events are suspected of being the result of this kind of attack, e.g., in June 2017, GPS receivers of several ships navigating in the Black Sea all derived the same incorrect position [7]. Besides, a jamming attack around an airport could prevent a plane and air traffic controllers from knowing its position and making take-off and landing operations difficult and unsafe. Several disruptions of this kind were reported in the past (e.g., [6, 20]).

3 Related Work

Both academia and industry have developed several systems for automatically detecting attacks on GNSS. In the signal processing domain, some of the pro-

posed algorithms include the monitoring of the receiver power spectrum (e.g., [21]), the Automatic Gain Control level (e.g., [22]), or the signal correlation peak (e.g., [23]). These solutions all imply access and modification of the receiver firmware [24] and thus increase the complexity of the detection method. The present work involves monitoring parameters easily accessible in RINEX files and therefore does not require any receiver update.

Many of the proposed systems also require the deployment of sensors (e.g., [21, 25]). Our research leverages the data from a network of stations already operating and can handily work on top of any existing station.

Moreover, to our knowledge, previous work focuses either on the jamming or the spoofing issue. In this study, we do not restrict the detection to a specific kind of attack but rather attempt to pinpoint any anomalous deviation from what is expected in terms of GNSS parameters.

The closest work to the present one is a recently published article [26], where anomalies in the C/N_0 measurements extracted from RINEX files are automatically detected to identify (unintentional) interferences. They do not target the discovery of intended disruptions. Their detection algorithm uses 15-minutes duration files and uncovers interference events lasting a few seconds. In this paper, we build an expectation of future observations based on days of history. This lets us believe that their system and ours would be complementary since we could detect longer events, e.g., a spoofing attack that slowly settles. Finally, their work addresses the C/N_0 parameter only, whereas we emphasize that our approach applies to other parameters.

Regardless of the differences between our work and the literature, it is worth mentioning that this research was *not* initiated by the wish of filling a gap in research with novel technology. Instead, it was motivated by the existence of an infrastructure (the AGNES network), available, delivering real-time and historical data in quantity, and the well-recognized need to improve the resilience of GNSS-dependent services. Robustness of defense calls for a diversity of protection mechanisms [27]. Our work demonstrates the value of GNSS reference stations as possible contributors to the set of solutions.

4 Data and Methodology

This section presents the available data and the methodology developed to process them and uncover anomalies within them. The complete procedure is summarized in Fig. 2.

4.1 Data

We study the data from AGNES, a network of static reference stations continuously tracking GNSS satellites, receiving signals, and storing measurements in RINEX files. For each station, those files are processed using the **G-nut/Anubis** software.² This tool, free and open-source for most of its functionalities, is

² <https://www.pecny.cz/gop/index.php/gnss/sw/anubis>.

designed to allow a quality check of GNSS observations. For each constellation and frequency tracked by a station, it provides a number of indicators (e.g., the C/N_0 per satellite, the mean C/N_0 over all satellites, a position solution) at the requested sampling rate (e.g., a data point per minute) and for the duration of the files given in input. These time series can then be analyzed with the system we developed to detect potential anomalies.

In this research, we focus on the data recorded during 2017, which include the signals received from GPS and GLONASS constellations, respectively on two different frequencies. This leads to the analysis of four different signals: GPS L1, GPS L2, GLONASS L1, and GLONASS L2. For each of them, we have at hand one time series per GNSS parameter, made of one data point per minute.

It is important to stress that in a CORS network, the stations' site locations are selected where the environment is favorable, i.e., there are as few topographic obstructions and reflective bodies as possible [28]. This means that the data collected have the benefit of being naturally relatively clean.

4.2 Indicator Selection

For the sake of simplicity, we decided to narrow down the research to a single indicator to handle univariate time series (i.e., the temporal sequence of a single variable). Our choice fell on the C/N_0 indicator (more precisely, the mean C/N_0 over all visible satellites' signals for each constellation and frequency). The procedure to detect anomalies outlined below can, however, be applied to other GNSS data parameter. A focus on the C/N_0 parameter is relevant for mainly two reasons. Firstly, this parameter would necessarily be affected in case of intentional interference (by definition) and potentially in a spoofing attack too. To succeed, a spoofer must indeed force its target to follow its forged signals. To that end, s/he might send signals with a stronger power. Therefore, a sudden increase in the recorded C/N_0 may indicate a spoofing attempt [29]. However, this technique would turn out ineffective if the attacker can increase the receiver noise power level simultaneously [30]. Secondly, when considering static stations, the C/N_0 patterns do not depend on other external quantities, as opposed to other measurements that would require incorporating additional data, e.g., ephemerides or weather data. This makes it a more straightforward parameter to study.

As a result of this choice, for a given station, the work essentially amounts to an anomaly detection performed on the mean C/N_0 , per minute over a year (i.e., 525 600 data points) for each of the four signals.

4.3 Anomaly Detection Scheme

There are generally two main ways to identify abnormalities in a system [31]. First, if some anomalies were already encountered in the past, their signatures can be captured. On that basis, one can verify if such patterns re-appear. The second method consists in learning the “profile of a normal behavior” in the data [32]. Anything that deviates too much from this normality can be considered an

anomaly. In the present research context, we do not have any signature of attack having targeted the network stations studied. We have the historical data of each station at our disposal but no knowledge on whether they were affected or not at some point. Besides, the outdoor simulation of attacks to generate signatures is complex, and such an experiment requires a license due to GNSS spectrum regulations. As a result, the second technique is preferred.

The challenge of this approach lies in the definition and modeling of this normal behavior. The decided strategy to this effect in our research is to build and validate a predictive model on historical data. It is the most common approach in univariate time series anomaly detection, according to [33].

The anomaly detection process we suggest thus takes place in three stages, as explained in Fig. 2. First, for a given data indicator such as the C/N_0 , a forecast model relying on the Seasonal and Trend decomposition using LOESS (STL) is trained to make accurate predictions. Second, future values for that indicator are predicted using that model. Finally, actual observations are compared to the predictions, and we decide whether they look normal or anomalous using a statistical rule based on the InterQuartile Range. We provide more details about the C/N_0 forecasting and statistical rule in the following sections.

Fig. 2. Proposed anomaly detection scheme on GNSS data for a given station. The time history of different parameters recorded by each station is easily accessible through RINEX files. A prediction-based anomaly detection can then be applied on a specific parameter's time series.

Carrier-to-Noise Ratio Forecasting

Model Selection. Since the GNSS satellites' trajectories repeat over time, the relative position between a static station and the satellites is periodically the same (every sidereal day for GPS, every eight sidereal days for GLONASS [8]). Consequently, a given signal's mean C/N_0 time series presents a seasonality, i.e., a pattern that repeats at regular intervals. It should be emphasized that this

would not necessarily be the case for a mobile GNSS receiver. The methodology we propose is intended for static receivers only.

The Seasonal and Trend decomposition using LOESS (STL) forecast model is selected for its ability to handle seasonal time series. Other more traditional methods, such as the SARIMA model, were considered. However, they appeared inappropriate for implementation reasons due to the high sampling rate of our dataset (a data point per minute) and the seasonal period value.

Introduced in [34], the STL algorithm uses a locally weighted regression (LOESS) to decompose a time series into three components: the trend, seasonal and residual components. Figure 3 presents an example of such decomposition applied on GPS L2 signal's mean C/N_0 time series over 15 days.

Fig. 3. STL decomposition applied on GPS L2 signal's mean C/N_0 time series on a duration of 15 days (2017 data). The upper graph shows the original signal. The three others respectively indicate the trend, the seasonal and residual components.

To obtain a forecast, the seasonal component is first estimated with STL and removed from the original time series. Predictions for the resulting *seasonally adjusted time series* are then made using an ARIMA model. Lastly, the seasonal component is added back to get final predictions [35].

The method involves a set of parameters that were optimized using a grid search. It should be noted that for simplicity, this optimization has solely been

conducted on the data gathered by a specific station. The mean absolute deviation (MAD) metric is used to quantify the prediction error.

Prediction Implementation Choices. Several decisions regarding which past data to use for the prediction tasks, how much, and the length of the period to predict (the *forecast horizon*) are presented and discussed in this section. The final setting is illustrated in Fig. 4.

Some models age well over time and do not need to be retrained (*static* models), while others require a continuous revision, i.e., they are *dynamic* [36]. In the case of GNSS data, a dynamic model is preferred. The solar activity is, for instance, a parameter that can influence the signals and that fluctuates over the years [37]. It would probably be inaccurate to make predictions for a given day using a model fitted on data from previous years. Therefore, a *rolling forecast approach* is adopted, where the model is updated for each new prediction.

Moreover, the amount of GNSS historical data for training the model should be large enough to capture the patterns. For the same reasons as just outlined, all history is certainly not relevant to predict the C/N_0 at a given minute. Two different sizes for the training set are experimented and compared, namely the past 7 and 31 days for GPS data, past 16 and 24 days for GLONASS (the difference between the constellations is due to the longer ground track repeatability of GLONASS satellites). Table 1 provided in the Appendix shows that in any case, the resulting error is almost equivalent. As the use of fewer past data is faster and allows to test the anomaly detection scheme on more data, the past 7 and 16 days are used for each prediction.

Finally, for a real-time anomaly detection system (which is the long-term goal of this research), predicting the next minute or next ten minutes would be appropriate. Nevertheless, to visually inspect the STL model performance, the forecast horizon is set to one day.

Fig. 4. Forecast implementation choices: illustration of the rolling forecast approach.

Hence, for a given signal, the previous 7 days (GPS) or 16 days (GLONASS) of mean C/N_0 provided per minute are used to predict values of the next day. The process takes around 1min for a GPS signal and 8min for GLONASS, so it could be performed in almost real-time as new data come. An example of prediction results for a randomly selected day on two signals is provided in Fig. 5. Predictions for each signal induce a MAD of 0.4201 dB-Hz regarding GPS L2 signal and a MAD of 0.4096 dB-Hz for GLONASS L1 signal. Given that the

mean C/N_0 of GPS L2 and GLONASS L1 signals over 2017 is on average 33.6203 dB-Hz and 46.1642 dB-Hz, the above MAD values should be considered as a good forecasting performance. For additional verification, predictions of other fifteen randomly selected days in 2017 with the same setting were made. The average prediction error for each signal is provided in Table 1, given in the Appendix. The results confirm the model's accuracy.

Fig. 5. Mean C/N_0 predictions per minute during one day for two types of signals, for a given station. The end of past data used for training the model appear in dark blue, predictions are highlighted in brown, true values are given in light blue. (Color figure online)

Statistical Rule. An anomaly should be declared when observations deviate significantly from the expectations provided by the predictive model. This implies the definition of a threshold above which the distance between an actual value and the estimated one (the prediction error) is not tolerable. For that purpose, the InterQuartile Range (IQR), defined as

$$IQR = Q3 - Q1, \quad (1)$$

is computed over the distances of the previous N predictions. The first quartile $Q1$ and the third quartile $Q3$ correspond respectively to the value under which

25% and 75% of the data lie. Anomalies are defined as observations whose distance to expectation falls below $Q1 - 1.5 \cdot IQR$ or above $Q3 + 1.5 \cdot IQR$. This is a commonly used rule in statistical-based anomaly detection, developed by [38]. Finally, we decide to inspect if collections of anomalies appear (as opposed to isolated anomalies). After flagging each prediction error as normal or anomalous, the density of anomalies is computed over a rolling window W . If more than k anomalies occur within W , the window is declared an *anomalous period*. Practically speaking, the predictions over the previous $N = 15$ days are used to compute the IQR. Thus, for any new station/receiver, only a few days would be necessary before the real-time detection process could start on incoming data.

5 Results

In this section, we first show the effectiveness of the procedure outlined above on a GPS signal using an event of reported accidental interference. Then, we present other anomalies successfully unveiled in the stations' data.

Fig. 6. True values of mean C/N_0 for GPS L2 signal (top figures), predictions of mean C/N_0 (second), MAD prediction error (third) and detected anomalous periods on the prediction error, highlighted in orange (lower figures). Each column of figures refers to one specific month. (Color figure online)

5.1 Proof of Effectiveness

The upper graph in Fig. 6 (a) shows the evolution of the mean C/N_0 per minute of GPS signals received on L2 frequency by a given station during March 2017. The C/N_0 observations seem regular. Predictions using the STL model are given in the second graph. Since the observations and predictions for these days are close, the corresponding prediction error represented in the third graph is low and stable. No anomaly is detected (lower graph).

On the other hand, in July 2017, unintentional interference in the GNSS frequency bands affected two stations of the AGNES network. In the upper graph of Fig. 6 (b), it can be observed that the mean C/N_0 parameter is indeed disturbed compared to the other days (perturbations are indicated with an orange brace). What is observed deviates from what was expected (provided in the second graph). The prediction error (third graph) consequently increases at the time of the interference. Those data points are identified as anomalous and are highlighted in the lower graph.

It should be noted that the occurrence of anomalies will bias the following predictions. Such behavior stems from selecting a rolling forecast approach and can already be seen in the presented case. The anomalous data should therefore be filtered before forecasting the following days.

This example confirms that we can effectively learn from a GNSS reference station's historical data to detect potential anomalous events. The monitoring of the distance between observed and expected values obtained through a predictive model indeed successfully reveals anomalies.

5.2 Detected Anomalies

The same procedure applied to the data collected by multiple AGNES network stations allowed discovering several anomalies in the mean C/N_0 behavior. Figure 7 shows four of them. At some point in time and during several hours, the mean C/N_0 experiences an unusual decrease compared to other days. The anomalies presented in (a) and (b) graphs affect the two GPS signals but only the GLONASS L1 signal. The ones in (c) and (d) affect all types of signals.

Interestingly, the disturbance in April 2017 was felt on stations 2 and 3, which are neighboring stations. Other cases of perturbations affecting two stations at a time were encountered.

Investigations with the CORS network operators revealed that those disturbances were caused by a snow accumulation on the stations' antenna. The reason why the GLONASS L2 signal was not affected by the anomaly exposed in Fig. 7 (a) and (b) still needs to be clarified. Although not being cases of intentional disturbances, those examples still highlight the detector's sensitivity to unusual events.

Fig. 7. Evolution of the mean C/N_0 on four types of signals for three stations during different periods of the year. The blue and orange curves correspond to signals from GLONASS constellation respectively on L1 and L2 frequencies. The green and red curves correspond to signals received from GPS satellites respectively on L1 and L2 frequencies. Anomalies were detected in these data and are indicated with an arrow. (Color figure online)

6 Limitations and Perspectives

The present research is subject to some limitations. To begin with, the STL prediction model appeared to be suitable, but other more recent and advanced forecasting methods could be considered instead, for instance, an autoencoder-based solution. It should be noted that the primary goal of this research was *not* to test every possible predictive model and find the perfect one for our data. Then, regarding the anomaly detection itself, the statistical rule to assess the observations' regularity should be refined. The addition of an “anomaly filter” step also constitutes a necessary enhancement. The detected anomalies should indeed not be taken into account for the following predictions.

Further research in automatic anomaly detection systems on GNSS data might consider investigating the following aspects. First, the same process could be repeated on other signals' parameters than the C/N_0 . It is very likely that monitoring multiple indicators simultaneously would improve the detection accu-

racy. The signals' Doppler shift, the satellites' orbital trajectories, and detected cycle slips in the signals' phase measurements are examples of such parameters. Besides, since several anomalies were found to affect two stations at a time, we believe that monitoring at the network level rather than station level by cross-referencing the stations' data could be another interesting area of study. The spatial relationships between the stations in the network have indeed not been exploited in the present work. Moreover, the anomaly detection scheme should be further applied to more recent data and data coming from the two other global constellations, i.e., Galileo and BeiDou. Finally, future work could be devoted to the simulation of attacks to evaluate the detection process in adversarial conditions.

7 Conclusions

Today, the dependency of critical infrastructures on GNSS is greater than ever. However, it is by design a fundamentally insecure technology that may be threatened in different ways, e.g., jamming or spoofing attacks. Therefore, it is imperative to monitor any anomaly that may be the sign of an attack attempt.

This paper presented how GNSS reference stations' data could be leveraged to that end. Specifically, training a predictive model on the past data for a given GNSS parameter allows encapsulating its normality profile and predicting what we expect to observe next. When the actual observations significantly deviate from those predictions, which is quantified by the prediction error, it indicates that the underlying data might be abnormal.

Besides its simplicity, this methodology offers the benefit of operating with high-level information from RINEX files and can therefore be easily applied to any static station's data easily without requiring hardware or firmware modification. Practically, only a few days of data are required in order to start the anomaly detection process. Moreover, it does not reduce to the detection of one specific human-made manipulation but rather aims to uncover any kind of irregular activity.

The effectiveness of such a detection scheme was demonstrated on the mean C/N_0 parameter using a reported case of unintentional interference. Finally, it allowed pinpointing other anomalies.

Acknowledgment. We would like to express our gratitude to PNAC and swipos teams from swisstopo, as well as SAPOS Baden-Württemberg and SAPOS Bayern for their valuable technical and logistic support during this research.

Appendix

Table 1. Average MAD error (expressed in dB-Hz) resulting from C/N_0 predictions over fifteen randomly selected days on GPS and GLONASS signals, using the STL forecast method. Comparison between the use of two sizes for the training set.

	GPS L1	GPS L2		GLONASS L1	GLONASS L2
7 days	0.4221	0.5266	16 days	0.6664	0.6930
31 days	0.4263	0.5316	24 days	0.69598	0.7527

References

1. United Nations Office for Outer Space Affairs page on Global Navigation Satellite Systems. <https://www.unoosa.org/oosa/en/ourwork/psa/gnss/gnss.html>. Accessed 11 May 2021
2. European Space Agency page on Precise Time Reference. https://gssc.esa.int/navipedia/index.php/Precise_Time_Reference. Accessed 11 May 2021
3. Analytica, O.: Global reliance on GPS creates new risks. Expert Briefings (2019). <https://doi.org/10.1108/OXAN-DB241765>
4. Homeland Security presentation: GPS Use in U.S. Critical Infrastructure and Emergency Communications. United States Technical Training Institute (USTTI). <https://www.gps.gov/multimedia/presentations/2012/10/USTTI/graham.pdf>. Accessed 10 May 2021
5. Cybersecurity and Infrastructure Security Agency, National Risk Management page on PNT. <https://www.cisa.gov/pnt>. Accessed 6 May 2021
6. New Jersey Star-Ledge: N.J. man fined \$ 32K for illegal GPS device that disrupted Newark airport system. https://www.nj.com/news/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html. Accessed 13 May 2021
7. Galileo GNSS: Mass GPS Spoofing Attack in Black Sea? <https://galileognss.eu/mass-gps-spoofing-attack-in-black-sea/>. Accessed 11 May 2021
8. Hofmann-Wellenhof, B., Lichtenegger, H., Wasle, E.: GNSS - Global Navigation Satellite Systems, 1st edn. Springer, Wien (2008). <https://doi.org/10.1007/978-3-211-73017-1>
9. Jin, S., Qian, X., Wu, X.: Sea level change from BeiDou navigation satellite system-reflectometry (BDS-R): first results and evaluation. Global Planet. Change **149**, 20–25 (2017)
10. European GNSS Global Navigation Satellite Systems Agency (GSA): GNSS User Technology Report, Issue 1 (2016)
11. Jones, M.: The civilian battlefield, protecting GNSS receivers from interference and jamming. Inside GNSS **6**, 40–99 (2011)
12. Petovello, M.: What is navigation message authentication? Inside GNSS (2018)
13. Jafarnia-Jahromia, A., Broumandan, A., Nielsen, J., Lachapelle, G.: GPS vulnerability to spoofing threats and a review of Antispoofing techniques. Int. J. Navig. Obs. (2012)
14. Ranganathan, A., Ólafsdóttir, H., Capkun, S.: SPREE, a spoofing resistant GPS receiver. In: MobiCom 2016: Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking, pp. 348–360, New York City (2016)

15. Neish, A., Walter, T.: Securing GNSS - a trip down cryptography lane. Inside GNSS (2020)
16. AZO - Space of Innovation story page: GNSS Jamming and Spoofing: Hazard or Hype? <https://space-of-innovation.com/gnss-jamming-and-spoofing-hazard-or-hype/>. Accessed 24 Aug 2021
17. Spirent white paper: GNSS Signal Spoofing: How to evaluate the risks to safety-critical and liability-critical systems (2020). <https://www.spirent.com/assets/white-paper-gnss-signal-spoofing>. Accessed 24 Aug 2021
18. Jansen, K., Schäfer, M., Moser, M., Lenders, V., Pöpper, C., Schmitt, J.: Crowd-GPS-Sec: leveraging crowdsourcing to detect and localize GPS spoofing attacks. In: 2018 IEEE Symposium on Security and Privacy, pp. 1018–103 (2018). <https://doi.org/10.1109/SP.2018.00012>
19. Bhatti, J., Humphreys, T.: Hostile control of ships via false GPS signals: demonstration and detection. *J. Inst. Navig.* **64**(1), 51–66 (2017)
20. Staff, T.: Disruption of GPS systems at Ben Gurion Airport resolved after 2 months. *The Times of Israel* (2019). <https://www.timesofisrael.com/disruption-of-gps-systems-at-ben-gurion-airport-resolved-after-2-months/>
21. Wende, J., Kurzhals, C., Houdek, M., Samson, J.: An interference monitoring system for GNSS reference stations. In: 15th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM), pp. 1–5. IEEE, Toulouse (2012)
22. Akos, D.M.: Who's afraid of the Spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *J. Inst. Navig.* **59**, 281–290 (2012)
23. Troglia Gamba, M., Truong, M.D., Motella, B., Falletti, E., Ta, T.H.: Hypothesis testing methods to detect spoofing attacks: a test against the TEXBAT datasets. *GPS Solutions* **21**, 577–589 (2017)
24. Schmidt, D., Radke, K., Camtepe, S., Foo, E., Ren, M.: A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Comput. Surv.* **48**(4), 1–31 (2016)
25. Proctor, A.G., Curry, C.W.T., Tong, J., Watson, R., Greaves, M., Cruddace, P.: Protecting the UK infrastructure: a system to detect GNSS jamming and interference. Inside GNSS Civilian Battelfield, 49–57 (2011)
26. Stader, J., Gunawardena, S.: Leveraging worldwide, publicly-available data to create an automated satnav interference detection system. In: Proceedings of the 2021 International Technical Meeting of The Institute of Navigation, pp. 69–83 (2021)
27. U.S. Department of Homeland Security (DHS) Science and Technology: Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework (2020). https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf
28. Intergovernmental Committee on Survey and Mapping: Guideline for Continuously Operating Reference Stations. Special Publication 1 (2014). <https://icsm.gov.au/sites/default/files/2018-02/Guideline-for-Continuously-Operating-Reference-Stations-v2.1.pdf>
29. Jafarnia-Jahromi, A., Daneshmand, S., Lachapelle, G.: Spoofing countermeasure for GNSS receivers, a review of current and future research trends. In: 4th International Colloquium on Scientific and Fundamental Aspects of the Galileo Programme, European Space Agency, Prague (2013)
30. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., Lachapelle, G.: GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/N0 observables. *Int. J. Satell. Commun. Network.* **30**(4), 181–191 (2012)

31. N-able blog page on Intrusion Detection System (IDS): Signature vs. Anomaly-Based. <https://www.n-able.com/blog/intrusion-detection-system>. Accessed 6 May 2021
32. Paulheim, H.: Lecture on anomaly detection. (2019) https://www.uni-mannheim.de/media/Einrichtungen/dws/Files_Teaching/Data_Mining_II/FSS2019/slides/DM03-AnomalyDetection-V1.pdf. Accessed 10 May 2021
33. Blázquez-García, A., Conde, A., Mori, U., Lozano, J.: A review on outlier/anomaly detection in time series data. *ACM Comput. Surv.* **54**(3) (2021)
34. Cleveland, R.B., Cleveland, W.S., McRae, J.E., Terpenning, I.J.: STL: a seasonal-trend decomposition procedure based on Loess. *J. Official Stat.* **6**(1), 3–33 (1990). <http://bit.ly/stl1990>
35. Hyndman, R.J., Athanasopoulos, G.: *Forecasting: Principles and Practice*, 3rd edn. Monash University, OTexts (2021)
36. Ebermann, T.: Time series prediction - a short introduction for pragmatists. <https://www.liip.ch/en/blog/time-series-prediction-a-short-comparison-of-best-practices>. Accessed 7 May 2021
37. Danson, E.: *Managing Solar Effects in GNSS Operations*. C&C Technologies (2011)
38. Tukey, J.W.: *Exploratory Data Analysis*. 1st edn. Addison-Wesley Pub. Co., Reading (1977)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.